TECHNICAL
REPORT

Evaluating the Security of the Global Containerized Supply Chain

Henry H. Willis, David S. Ortiz

RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT

TECHNICAL REPORT

Evaluating the Security of the Global Containerized Supply Chain

Henry H. Willis, David S. Ortiz

INFRASTRUCTURE, SAFETY, AND ENVIRONMENT

Preface

A global supply chain links the United States and its economy to the rest of the world. The unit of measure of the supply chain is the shipping container: a sturdy steel box of standard dimensions that carries most freight. Millions of containers circle the earth on specialized ships, railcars, and trucks. Actions to ensure the security of the system of containers and their conveyances have traditionally focused on preventing smuggling and theft. Since September 11, 2001, supply-chain security has been redefined as preventing terrorists from targeting the containerized supply chain or transporting a weapon in a shipping container. The change in focus raises questions about the effectiveness of proposed security efforts and the consequences they may have for supply-chain efficiency.

This report outlines a framework for assessing and managing supply-chain security and efficiency. It identifies key stakeholders in the system, defines critical capabilities of the supply chain, and reviews current efforts to improve supply-chain security and efficiency. This framework also defines a path for future research and is to be the first of a series of studies on the topic of supply-chain security. The results of this study will be of interest to public and private decisionmakers responsible for policies and investments to manage components of the supply chain.

This report results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by donors and by the independent research and development provisions of RAND's contracts for the operation of its U.S. Department of Defense federally funded research and development centers.

Contents

Preface iii
Figures and Tables vii
Summary ix
Abbreviations xv

SECTION 1
Motivation and Introduction: Toward a Model for Assessing Supply Chain Security 1

SECTION 2
Proposed and Implemented Security Measures Since September 11, 2001 4
Customs-Trade Partnership Against Terrorism 4
Operation Safe Commerce 4
The Container Security Initiative 4
The Maritime Transportation Security Act of 2002 5
Antitamper Seals 5
Radio-Frequency Identification 5
X-Ray and Gamma-Ray Scanning 5
Radiation Pagers, Portal Sensors, and Remote Monitoring 6

SECTION 3
The Global Supply Chain: Points of View, System Components, and Stakeholders 7
The Transaction Layer: A Business Fulfillment Network 8
The Logistics Layer: A Multimodal Physical Network for the Transport of Cargo 10
The Oversight Layer: The Legal and Regulatory Structure of the Global Supply Chain 12
Interactions Among Layers in the Supply Chain 13

SECTION 4
Capabilities of the Global Container Supply Chain 16

SECTION 5
Managing Container Shipping Security: A Case of Technology-Induced Risk 18
Building Supply-Chain Capabilities 18
Customs-Trade Partnership Against Terrorism: Making Supply-Chain Participants Responsible for the Security of Container Cargo 19
Operation Safe Commerce: Harnessing Technology to Improve Customs Inspection Effectiveness 19

Container Security Initiative: Increasing Deterrence and Efficiency Through Cargo Inspection at Foreign Ports 21
Maritime Transportation Security Act: Reducing Theft and Improving Incident Response at Ports and on Vessels 21
Antitamper Seals: Improving the Integrity of Container Shipping 21
Radio Frequency Identification: Improving the Transparency of Supply-Chain Networks 22
X-Ray and Gamma-Ray Scanning: Improving Transparency of Cargo Shipments 22
Radiation Pagers, Portal Sensors, and Remote Monitoring: Increasing Capabilities to Detect Weapons of Mass Destruction 22

SECTION 6
Preliminary Conclusions, Recommendations, and Future Inquiry 23
Preliminary Conclusions 23
The Inseparability of Supply-Chain Security and Efficiency 23
Potential Underinvestment in Fault Tolerance and Resilience 25
Recommendations 26
The Public Sector Should Seek to Bolster the Fault Tolerance and Resilience of the Logistical Supply Chain 26
Security Efforts Should Address Vulnerabilities Along Supply-Chain Network Edges 26
R&D Should Target New Technologies for Low-Cost, High-Volume Remote Sensing and Scanning 26
Future Inquiry 27

References 29

Figures and Tables

Figures

S.1. Interactions Between the Logistics, Transaction, and Oversight Layers of the Supply Chain x
1. The Business Transaction Network 9
2. The Supply Chain Seen in Terms of People and Places 11
3. Interactions Between the Logistics, Transaction, and Oversight Layers of the Supply Chain 14

Tables

S.1. Organizational Interests x
S.2. Examples of How Preparedness Strategies May Influence the Exposure-Effects Chain of Notional Terrorist Events xii
1. Organizational Interests 14
2. Examples of How Preparedness Strategies May Influence the Exposure-Effects Chain of Notional Terrorist Events 20

Summary

The global supply chain is the network of suppliers, manufacturing centers, warehouses, distribution centers, and retail outlets that transforms raw materials into finished products and delivers them to consumers (Simchi-Levi, Kaminsky, and Simchi-Levi, 2002). Security of the system has traditionally focused on reducing shrinkage—the loss of cargo shipments through theft and misrouting. However, heightened awareness of terrorism has redefined supply-chain security—the consequences of an attack on or via a critical global port could be a tremendous loss of life and a crippling of the U.S. economy—and has brought increased attention to the risks containerized shipping presents.

The response has been proliferation of new security measures. For all these efforts, is the system of trade more or less secure? Will we know if these efforts are successful? How will success or failure be measured? This report presents a strategy for answering these questions using methods for managing risk of large-scale systems to analyze the structure of the container supply chain and its properties.

The Three Layers of the Global Container Supply Chain

The structure of the global container supply chain would seem self-evident: It is a system of vessels, port facilities, railcars, trucks, and containers that transport goods in discrete units around the earth. That view, however, pertains only to the physical components of a system that includes the cargo, information, and financial flows required for the system to operate. We propose viewing the supply chain as three interdependent and interacting networks: a physical logistics system for transporting goods; a transaction-based system that procures and distributes goods and that is driven primarily by information flows; and an oversight system that implements and enforces rules of behavior within and among the subsystems through standards, fines, and duties. Network components are *nodes*, such as factories and ports, and *edges*, such as roads and information links. Figure S.1 illustrates the subsystems as a collection of layers. The oversight system has agencies and organizations that interact with the layers of the global container supply chain. The different points of view of the supply chain can be viewed in terms of a layered set of networks. The *logistics layer* is responsible for the movement of cargo along a network of roads; the *transaction layer* orders goods and materials from a network of suppliers; and the *regulatory layer* specifies standards for operation within its area of authority.

Table S.1 lists examples of the organizations present in each layer. The three layers may be specified by the organizations that comprise each. Note that oversight agencies have a limited range of influence over organizations in either the transaction or logistics layer.

Figure S.1
Interactions Between the Logistics, Transaction, and Oversight Layers of the Supply Chain. The different points of view of the supply chain can be viewed in terms of a layered set of networks. The logistics layer is responsible for the movement of cargo along a network of roads; the transaction layer orders goods and materials from a network of suppliers; and the regulatory layer specifies standards for operation within its area of authority.

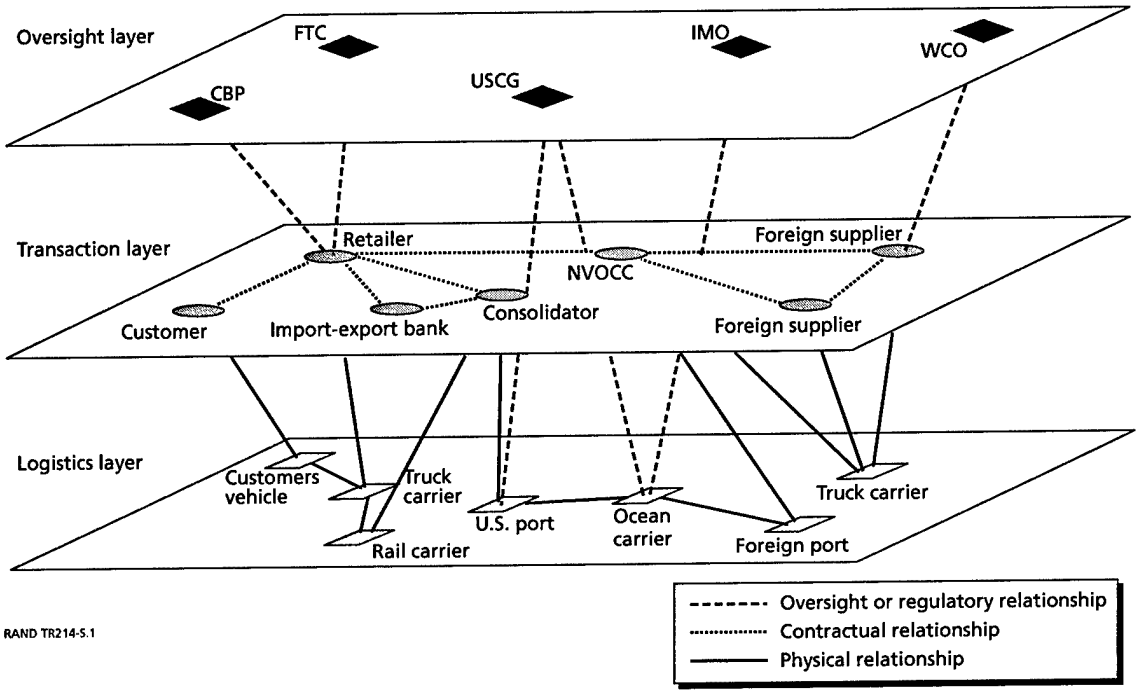


Table S.1
Organizational Interests. The three layers may be specified by the organizations that comprise each layer. Note that oversight agencies have a limited range of influence over organizations in either the transaction or logistics layer.

Layer	Examples of Stakeholders	Examples of Oversight Agencies
Transaction	Wal-Mart Target Ford Non–Vessel-Operating Common Carriers (NVOCCs)	Federal Trade Commission U.S. Customs and Border Protection World Customs Organization
Logistics layer	International Longshore and Warehouse Union Pacific Maritime Association International Labor Organization CSX Transportation APL Maersk Sealand Port of Long Beach	U.S. Department of Labor U.S. Department of Homeland Security Local law enforcement U.S. Coast Guard U.S. Customs and Border Protection World Customs Organization

Examining the supply chain from each of these perspectives yields insights into the concerns of relevant stakeholders, the levers available to improve supply-chain performance, and the interactions among the layers that improve or detract from system performance.

Capabilities of the Global Container Supply Chain

The ability of the global container supply chain to deliver goods efficiently and securely can be described through five measurable capabilities:

- **Efficiency.** Container shipping has evolved primarily to deliver goods more quickly and more cheaply than other modes of transport, when volume and mass are taken into account.
- **Shipment reliability.** Supply chains must behave as expected, retrieving and delivering goods as directed, with a minimum amount of loss due to theft and accident.
- **Shipment transparency.** The goods that flow through a supply chain must be legitimately represented to authorities and must be legal to transport.
- **Fault tolerance.** The container shipping system should be able to respond to disruptions and failures of isolated components without bringing the entire system to a grinding halt.
- **Resilience.** A supply chain is resilient insofar as it is able to return to normal operating conditions quickly after the failure of one or more components. Resilience is a function of both the system's design and the responsiveness of the oversight layer.

The efficiency of the container shipping system is measured in terms of its speed and cost, taking reliability into account. Security, however, is a function of the final four capabilities. Efficiency and security are often portrayed as in direct conflict, but in our formulation, they are measured differently and may support or hinder one another, depending on the circumstances. Analysis of any program's efficiency and security implications needs to consider the system under both normal and emergency operating conditions.

Managing Risk in the Global Container Supply Chain

We applied a framework of technology-induced risk assessment (Morgan, 1981) to provide insight into how supply-chain security capabilities are realized. Table S.2 details how policy and technology proposals support improved supply-chain capabilities. This table presents the perspective of capabilities that could be captured by private shippers, carriers, and port operators and by the U.S. government. Through application of this methodology, we also get a high-level view of how these objectives come together as an integrated container security strategy. The methodology also reveals gaps in the set of policies intended to improve the security of the global container supply chain: fault tolerance and resilience, for instance, have received little attention from policymakers.

Table S.2
Examples of How Preparedness Strategies May Influence the Exposure-Effects Chain of Notional Terrorist Events

			Anticipated Supply Chain Security Effects			
			Threat or Vulnerability Reduction		Consequence Reduction	
Policy or Technology	Driving Layer	Anticipated Supply Chain Efficiency Effects	Reduce Probability of Attack	Reduce Probability of Successful Attack	Avoid or Modify Attack Consequences	Mitigate or Compensate for Consequences
Customs-trade partnership against terrorism	Transaction and logistics	Reduced shipping cost and time and increased volume: *Expedited customs*	Reduced damage, losses, and fraud: *Deter terrorists, thieves, and smugglers*			
Operation Safe Commerce	Logistics and oversight			Reduced fraud: *Detect at entry*		
Container security initiative	Oversight			Reduced damage and fraud: *Detect at origin*		
Maritime Transportation Security Act of 2002	Oversight			Reduced theft: *Control access*		Increased Fault tolerance and resilience: *Disaster planning*
Anti-tamper seals	Transaction and logistics			Reduced damage: *Detect at origin* Reduced fraud: *Detect at origin or entry*		
Radio frequency identification	Transaction and logistics	Reduced shipping cost and time: *Improved Logistics*		Reduced theft losses: *Detect unapproved transport* Reduced damage: *Detect at origin* Reduced fraud: *Detect at entry or origin*		Increased resilience: *Rapid location and rerouting of shipments following a disaster*
X-ray and gamma-ray inspection	Logistics and oversight			Reduced damage: *Detect at origin* Reduced fraud: *Detect at origin or entry*		
Radiation pagers, portal sensors, and remote monitoring	Logistics and oversight			Reduced damage: *Detect at origin*	Reduced damage: *Detection before cargo enters ports*	

Preliminary Conclusions

Applying the layered capabilities framework to the analysis of current efforts to improve supply-chain security led us to two conclusions:

- **Supply-chain efficiency and security are distinct but interconnected.** Efforts to improve the efficiency of the container shipping system may or may not have affected the security of the system. In turn, security efforts might also improve efficiency. Those that do not may lead to unexpected negative consequences as the system adapts to compensate for or work around resulting losses of efficiency.
- **Both public- and private-sector initiatives to improve the security of the global supply chain have focused largely on preventing and deterring smuggling and terrorist attacks.** These initiatives focus on improving the transparency of the global container supply chain. Few initiatives have focused on improving the fault tolerance or resilience of the system, which could be a fruitful area for new security measures.

Recommendations

These conclusions suggest three complementary paths for improving the security of the global container supply chain while maintaining its efficiency:

- **The public sector should seek to bolster the fault tolerance and resilience of the global container supply chain.** The closure of a major port—for whatever reason—would have a significant effect on the U.S. economy. The federal government should lead the coordination and planning for such events for two reasons. First, the motivation of the private sector to allocate resources to such efforts is subject to the market failures of providing public goods. Second, the government will be responsible for assessing security and for decisions to close and reopen ports.
- **Security efforts should address vulnerabilities along supply-chain network edges.** Efforts to improve the security of the container shipping system continue to be focused on ports and facilities (although many ports around the world still failed to meet International Ship and Port Security Code guidelines even after the July 1, 2004, deadline.) Unfortunately, the route over which cargo travels is vast and difficult to secure. Measures to keep cargo secure while it is en route are essential to a comprehensive strategy to secure the global container supply chain.
- **Research and development should target new technologies for low-cost, high-volume remote sensing and scanning.** Current sensor technologies to detect weapons or illegal shipments are expensive and typically impose significant delays on the logistics system. New detection technologies for remote scanning of explosives and radiation would provide valuable capabilities to improve the security of the container shipping system.

Future Inquiry

This report is our initial assessment of the security of the global container supply chain; our work is continuing in the following areas:

1. assessment of policies for improving supply-chain security
2. systems analysis of supply-chain risk
3. technology assessment and research and development planning for improving supply-chain performance
4. economic analysis of global trade trends on supply-chain performance.

Abbreviations

BE	bill of exchange
CBP	U.S. Customs and Border Protection
CIS	U.S. Citizenship and Immigration Services
CSI	Container Security Initiative
CSX	CSX Transportation
C-TPAT	Customs-Trade Partnership Against Terrorism
FTC	Federal Trade Commission
GAO	General Accounting Office
IB	import bank
IMO	International Maritime Organization
MTSA	Maritime Transportation Security Act
NVOCC	Non–Vessel-Operating Common Carrier
OECD	Organisation for Economic Co-Operation and Development
OSC	Operation Safe Commerce
POLB	Port of Long Beach
RFID	radio frequency identification
SB	seller's bank
TAPA	Technology Asset Protection Association
TSA	Transportation Security Administration
USCG	U.S. Coast Guard
WCO	World Customs Organization

SECTION 1

Motivation and Introduction: Toward a Model for Assessing Supply Chain Security

The global supply chain is an international system that has evolved to make the transport of freight throughout the world amazingly efficient. The chain consists of the suppliers, manufacturing centers, warehouses, distribution centers, and retail outlets that move raw materials, work-in-progress inventory, and finished products from producer to consumer (Simchi-Levi, Kaminsky, and Simchi-Levi, 2002). The shipping container and its transport system are integral components of the global supply chain.

Approximately 90 percent of the world's cargo is shipped via container, including 75 percent (by value) of non-North American trade to and from the United States (Stana, 2004). There are approximately 18 million containers of various sizes around the world. The standard container is a 20-ft equivalent unit, which is a sturdy steel box measuring 20 × 8 × 8 ft, although containers are often 40 ft long and can come in various configurations to support different kinds of cargo (Pollack, 2004). These containers are bolted to the chassis of trucks, stacked two high on flatbed railcars, and packed onto ships as large as aircraft carriers carrying thousands of such containers. Port operations and technology are optimized so that ships spend a minimum amount of time at the quay and the maximum time en route.

The principal concern of business is to increase the efficiency of the global supply chain, paying comparatively little attention to security. In recent years, ocean carriers have cut crews to an absolute minimum and have continued to order larger and faster ships in an effort to squeeze every cent of profit from the system (Pollack, 2004).

Prior to September 11, 2001, supply-chain security focused primarily on reducing shrinkage—the loss of cargo shipments through theft and misrouting. This risk motivated action in the private sector. In 1997, 60 high-technology companies collaborated in the Technology Asset Protection Association (TAPA) (Flynn, 2000). These firms are consumer electronics and computer manufacturers and retailers, for whom theft represents a considerable business risk. TAPA developed and issued guidelines for shipping security for these products, and "if a freight forwarder or carrier wants to do business with any of TAPA's well-heeled members, they must adopt these practices" (Flynn, 2000). TAPA now includes European members, and it issues security requirements and self-evaluation tools to potential service providers.[1]

The problems of theft and smuggling demonstrate the relative ease with which criminal elements have capitalized on the use of containers as conveyances. Anonymity of contents, opaque ownership arrangements for vessels, and corruption in foreign ports have all facilitated the efforts of those who are inclined to use container shipping for illegal purposes.

[1] Documentation is available on TAPA's Web site (TAPA, 2004).

More recently, the private sector has looked to new technologies for solutions for improving supply-chain efficiency and reducing shrinkage. Wal-Mart, for example, has mandated that its suppliers use radio-frequency identification (RFID) tags to increase the visibility of the shipping and purchasing process and to improve the efficiency of the supply chain; in the case of drug shipments, it is also hoped that the tags will help combat counterfeiting (Feder, 2004). The Smart and Secure Tradelanes Initiative consortium applies RFID technology at the container level, and in its initial report, it notes that current supply-chain processes are engineered for efficiency, productivity, and flexibility, with minimal emphasis on security. To the extent that security is a consideration, it is focused on reducing cargo theft and protecting proprietary data from competition (Smart and Secure Tradelanes, 2003).

Heightened awareness of terrorism has redefined supply-chain security and increased attention to the risks containerized shipping presents. The west-coast port lockout of 2002 suggested the magnitude of economic effects a terrorist-related event might cause. Estimates placed the losses for the ten-day lockout between $4.7 billion and 19.4 billion (Iritany and Dickerson, 2002; Cohen, 2002).

Steven Flynn of the Council on Foreign relations has been among the most vocal proponents of heightening the security of the international supply chain. He writes that a terrorist organization could easily ship people, arms, or even a weapon of mass destruction in a standard cargo container (Flynn, 2004). Given that over 7 million containers enter the United States every year through its seaports and that few of these containers are physically inspected, the containerized shipping system seems to present an attractive target (GAO, 2003).[2] The magnitude of the system and its unparalleled passion for efficiency at all levels support Flynn's hypothesis. Security experts believe it is only a matter of time before the United States or one of its allies is the victim of a terrorist attack using a shipping container, resulting in significant loss of life and in widespread and global economic damage.

Since September 11, 2001, emphasis on port and maritime security has increased. The International Maritime Organization (IMO) has updated the International Ship and Port Security code to require port, carrier, and vessel security plans and personnel. The United States has responded with parallel legislation in the form of the Maritime Transportation Security Act of 2002 (MTSA), which requires similar actions for U.S. ports and vessels and appoints the U.S. Coast Guard (USCG) as the organization responsible for compliance and enforcement. The World Customs Organization, the World Shipping Council, the Pacific Maritime Association, the United Nations Council on Trade and Development, U.S. Customs and Border Protection (CBP), the Transportation Security Administration (TSA), and every one of the 361 U.S. ports and most international ports have all initiated responses.

The urgency of these responses is justified by the gravity of the potential for loss of life if terrorists were able to use the container shipping system successfully. However, for all these security efforts, is the system of trade more secure? How insecure was it in the first place? Will we know if these efforts are successful? How will success or failure be measured?

The costs and scale of security measures to counter this threat demand analysis of what other effects such attacks might have and how the security measures themselves affect performance of the container shipping system. This report presents a framework for answering these questions.

---

[2] Some U.S.-bound containers arrive at Canadian ports, entering the United States via truck or rail.

Our discussion is organized as follows. Section 2 describes security measures that have been implemented or proposed since September 11, 2001. Section 3 depicts three perspectives on the supply chain: (1) a logistics network of roads, tracks, and sea-lanes that moves cargo from an origin to a destination; (2) a transaction network linking buyers, sellers, and their financial intermediaries; and (3) an oversight system regulating operation of the logistics and transaction networks to protect public safety and levy tariffs. These perspectives represent three interconnected layers of networks and identify stakeholders in different stages of the supply chain. They also illustrate the levers available for realizing improved supply-chain security and efficiency. Section 4 defines the capabilities of a secure and efficient supply chain.

Building on these descriptions of the containerized shipping system, Section 5 lays out a framework for assessing and managing supply-chain security. Drawing from literature on technology-induced risk, we examine current security approaches and policies from the perspective of how they affect supply-chain capabilities and which stakeholders they involve. Finally, we close with a discussion of insights that this risk assessment framework provides about current port security efforts and future directions for research to support policymaking to protect U.S. ports, trade lanes, and the container supply chain.

Our focus is on U.S. domestic policies for the operation of ports and maritime vessels as nodes in the global container supply chain; we have limited ourselves to this subset of the global container supply chain because it has been the subject of the majority of proposed measures for protecting the security of containerized shipping in the face of the terrorist threat. Future analysis will address the system in general, including its global nature and the security issues related to intermodal transport.

SECTION 2

Proposed and Implemented Security Measures Since September 11, 2001

The response to the terrorist threat to container shipping has been multifaceted. It has involved evaluation and adoption of new technologies, passage of new regulations, and implementation of new operating processes and protocols. To date, most efforts have concentrated on maritime shipping operations (as opposed to intermodal transport). The focus on seaports has occurred for two principal reasons: Seaports are America's principal connections to the global economy, and seaports are bottlenecks in the system at which it is possible to impose additional security provisions. This section presents an overview of some major U.S. and international initiatives and technologies to improve supply-chain and port security taken since September 11, 2001. We will refer to these initiatives as we develop our analytical framework.

Customs-Trade Partnership Against Terrorism

The goal of Customs-Trade Partnership Against Terrorism (C-TPAT) is to push responsibility for cargo security onto stakeholders in the supply chain. C-TPAT is a voluntary program that shippers and carriers can enter to assure CBP that they have put into place the best security practices for the packing, tracking, and distribution of all containers and goods en route to the United States. In return, shippers and carriers are rewarded through quicker processing and reduced probability of inspection delays (CBP, 2004).

Operation Safe Commerce

Operation Safe Commerce (OSC) is a technology-development and -deployment program intended to improve the ability of customs agents to detect illicit cargo on its entry into a port. According to TSA (2004), "OSC is a collaborative effort between the federal government, business interests, and the maritime industry to develop and share best practices for the safe and expeditious movement of containerized cargo." Through a set of grants, OSC is promoting the testing, evaluation, and fielding of container scanning and tracking technologies.

The Container Security Initiative

The Container Security Initiative (CSI) inspects and clears containerized cargo before shipment to the United States (CBP, undated). Through this program, CBP has deployed

inspectors at 19 of the world's major seaports in Europe, Asia, Africa, and North America. The goal of CSI is to make it more difficult to transport illegal shipments to the United States by implementing inspections at ports of origin, thus increasing U.S. security. Although CBP has offered to station foreign customs inspectors at U.S. ports, none have accepted to date.

The Maritime Transportation Security Act of 2002

MTSA dictates that domestic ports and carriers with U.S.-flagged vessels develop and institute port, port area, and vessel security plans and register these plans with the USCG (MTSA, 2002). These requirements establish standards and protocols for port security, inspections, and emergency response. MTSA is the U.S. version of the IMO's International Ship and Port Security Code (IMO, 2004).

Antitamper Seals

Antitamper seals are a broad set of technologies that detect and indicate when an unauthorized party has opened a container. They range from electronic devices that record when and by whom containers are opened to proposals to mark containers with unique "fingerprints" that are modified when a container is opened or compromised. Even the simplest antitamper seals, such as high-quality cable seals, are considerably more expensive than common bolt seals.

Radio-Frequency Identification

RFID technologies allow shippers and carriers to track cargo while it is within the container shipping system. The devices can record and transmit information about a container's origin, destination, contents, or processing history. RFID systems are typically designed to transmit information about cargo when the shipment passes salient portals, such as entry or exit from a port or when the cargo is loaded or unloaded from a ship.

RFID devices are available as both passive and active technologies. Passive devices transmit only when in the presence of a reader that provides the required power. They have ranges up to a few meters and are typically used to track shipments at the unit or carton level. Active devices are battery powered and can transmit over distances as far as 100 m or more. Thus, active devices have been applied to tracking cargo at the container and pallet levels.[3]

X-Ray and Gamma-Ray Scanning

X-ray and gamma ray technologies are used to scan containers for misrepresented or illegal shipments. These technologies allow CBP to visualize for nonintrusive inspections of a con-

[3] Bear-Stearns has issued several analyses of RFID technology and solutions providers (Alling, Wolfe, and Brown, 2004; Wolfe et al., 2003).

tainer' contents, obviating the need to open it and inspect the contents physically. Currently, between 5 and 6 percent of containers are inspected either intrusively or nonintrusively (Wasem et al., 2004). Application has been limited because of the cost of the machines, the lack of space at ports, the time required to scan, and the relatively high false-positive rates that result from the inconclusive visualizations that the technologies provide (Stana, 2004).

Radiation Pagers, Portal Sensors, and Remote Monitoring

Technologies for the remote sensing of weapons of mass destruction are under development. Radiation pagers are portable devices that can be used to detect nuclear or radiological weapons as inspectors move throughout a port or vessel. Portal sensors are designed to detect weapons of mass destruction as containers enter and leave ports or vessels. These and other remote-monitoring devices to detect weapons of mass destruction and other illegal cargo are in early development. However, capabilities are expected to improve over time and possibly be integrated with RFID or other container tracking technologies.

SECTION 3

The Global Supply Chain: Points of View, System Components, and Stakeholders

Section 1 discussed the global supply chain generally as the system of containers and conveyances in which and on which goods flow from producers to consumers. This view is too coarse to permit a formal analysis of the properties of the supply chain. In fact, there are several ways in which to characterize the system, each with unique properties and performance measures.

To a product-based business, the supply chain is its network of suppliers and subsuppliers. This *transaction layer* connects participants to each other legally through contracts, informationally through product specifications, financially through transaction records, and physically through the actual product or good.

The delivery system, the *logistics layer*, is a conveyance through which products move. The system of roads, tracks, and sea-lanes and the containers that flow along them comprise a network, one that provides services to the producers and consumers of goods. Members of the business community would prefer that the physical system be transparent, that a financial transaction plus an associated waiting time be all that is required to guarantee the movement of products, the particular truck, train, or boat not being of consequence (World Shipping Council, 2003).

An *oversight layer*, consisting of customs organizations, law enforcement, and national and international bodies, oversees the contracting for and movement of goods. At times, the oversight bodies work within a particular layer of the supply chain: USCG guarantees maritime safety and security, and the Federal Trade Commission (FTC) monitors the actions of firms to ensure compliance with trade law. At other times, the organization must interact with both layers: CBP is responsible for the collection of duties and for helping to ensure port security.

The transaction, logistics, and oversight layers of the supply chain each form a network.[4] For example, in the logistics layer, the *nodes* are all facilities through which the cargo

[4] The flow of goods on networks is a mature topic in logistics (Ford and Fulkerson, 1962). More recently, researchers have studied the structure and dynamics of social, physical, and transportation networks (Watts, 1999; Holmes, 2004). An edge in a social network may be represented by a business relationship between two firms: Goodyear supplies tires to General Motors, for example. Two properties of networks concern us in this study: the small-world phenomenon and the property of "connectedness." A *small world* is a network that has relatively few edges leading to and from the average node but that has a small number of successive edges that connect any two nodes. The most famous example is the notion that there are "six degrees of separation" between any two humans (Guare, 1990). Small-world phenomena have been demonstrated in the electric power grid, the Internet, and in the nervous systems of animals (Watts, 1999). Intuitively, one would think that the nodes with the most edges are responsible for reducing the number of "jumps," but this is not the case: It is the nodes that connect two so-called well-connected nodes that guarantee the small-world phenomenon (Watts, 1999). *Connectedness* is the property of a network that all nodes are connected to all other nodes through a set (or sets) of edges. These properties together govern the resilience of the system. Amaral et al. (2000) studied several types of small-world networks and showed that certain types of networks are able to better maintain connectedness in the face of attacks on nodes and edges than are

travels from origin to destination, and the *edges* (i.e., the links that connect nodes) are the roads, railroad tracks, and sea-lanes on which the cargo moves. Examination of the supply chain from each of these perspectives yields important insights into both the concerns of relevant stakeholders and the levers available to improve supply-chain performance.

The Transaction Layer: A Business Fulfillment Network

For a company, the supply chain is the collection of individuals or firms that supply material for the production or sales of a product. The supply chain for a cookie manufacturer would, at a minimum, include suppliers of butter, flour, sugar, flavorings, and packaging. These suppliers are held to performance standards for their products and for delivering them subsequent to an order: The butter must have a certain percentage of milk fat; when an order is placed, the supplier is expected to fill the order and deliver the butter within a specified time. The cookie manufacturer should have little concern for the particular route that the butter took from its supplier, only that it arrived within a prespecified window of time.[5] The relationships between the manufacturer and its suppliers are based on legal contracts for the fulfillment of orders.

This transaction-based view of the global supply chain can be represented as the union of two interacting networks: an information network and a material network. The information network coordinates the flow of goods and payments and is regulated by U.S. and international trade law. The material network for a particular firm includes all direct and indirect suppliers of goods. Failures of nodes in the transaction layer are fundamentally different from failures in the logistics layer described in the next section.

The transaction layer views the logistics layer as a conveyance mechanism. A failure in the transaction layer eliminates the source of a product or the financial flows that trigger logistics demands; a failure in the logistical system limits the flow of goods through a particular port, rail yard, or truck stop or along a particular route. For example, a disruption to a supplier of polo shirts—a node in Wal-Mart's supply chain—is fundamentally different from a disruption to a seaport—a node in the logistics layer. The disruption to the garment factory affects its suppliers and customers, but a disruption to a port affects all cargo that would have passed through it, polo shirts and automobiles alike, with far greater economic consequences. Figure 1 illustrates the contracting and payment mechanism among the seller, the seller's bank, the import bank, and the buyer for a bill of exchange for goods (Organization for Economic Cooperation and Development [OECD], 2003), the goods pass through the logistics layer, represented as a gray bar in the center of the figure.

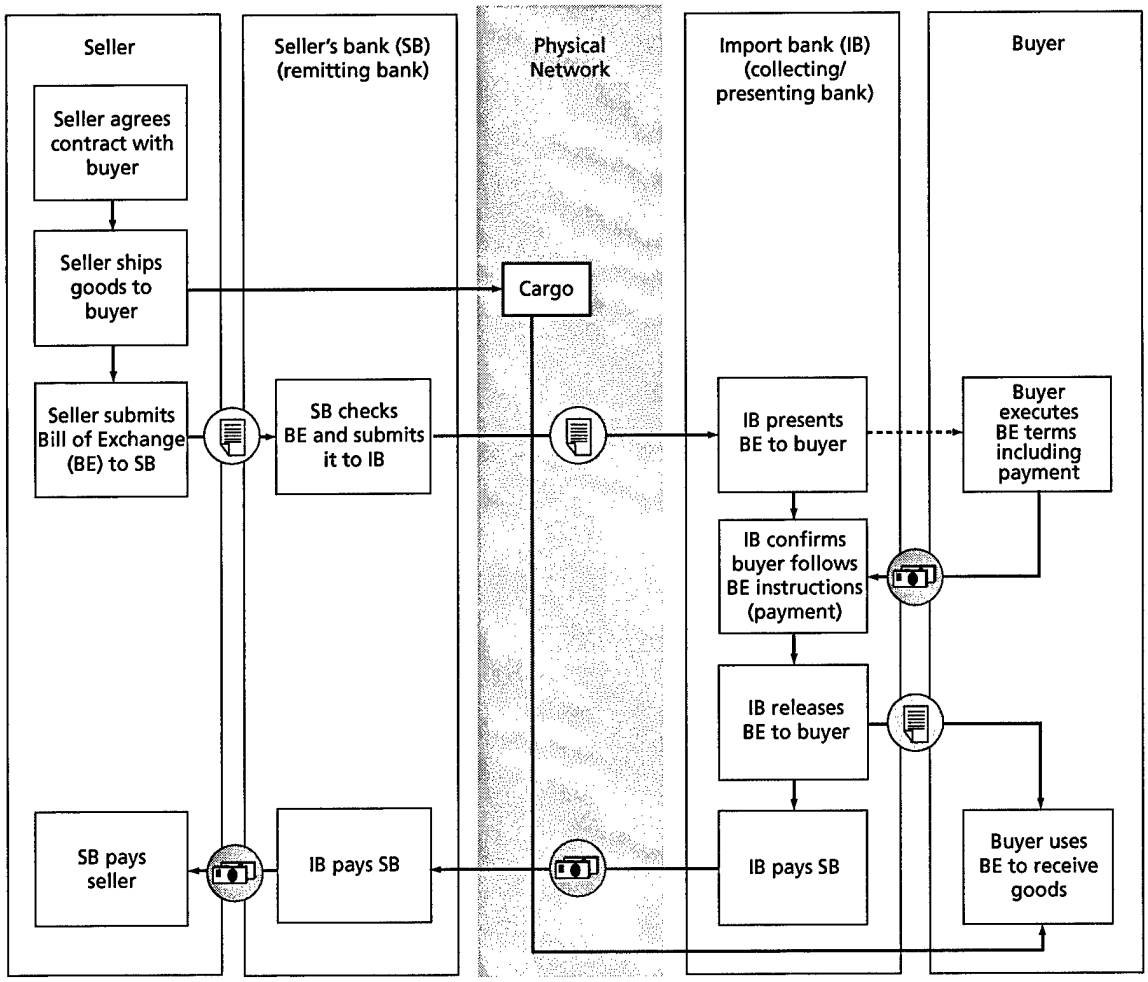
The business layer has been used to improve supply-chain performance in several ways. First, companies searching for a competitive advantage have become early adopters of technologies and policies to improve supply-chain security and efficiency. The Smart and Secure Tradelanes Initiative is one such example: A consortium of technology vendors, shippers, and port operators is evaluating technologies and processes to increase network transparency to reap the presumed security and efficiency benefits (OECD, 2003).

---

others. We will appeal to network-theoretic notions throughout this work, but we will not directly assess the network properties of the international supply chain in this analysis.

[5] This is not always the case: Wal-Mart monitors all costs diligently and recently rerouted Chinese cargo from Hong Kong to Guangdong to save $650,000 annually on shipping (Cleeland, Iritany, and Marshall, 2003).

Figure 1
The Business Transaction Network. The transaction that results in the shipments of goods from a seller to a buyer and the exchange of funds between the buyer and seller sees the logistic network as a conveyance for products. This illustrates the contracting and payment mechanism among the seller, the seller's bank, the import bank and the buyer for a bill of exchange for goods.



SOURCE: OECD, "Security in Maritime Transport: Risk Factors and Economic Impact," Maritime Transport Committee report, 2003. Online at http://www.oecd.org/home/ (as of November 5, 2003). Adapted and used with permission.

Second, organizations with market power have used the business layer to demand improved supply-chain security. For example, Wal-Mart and the Department of Defense have demanded that their largest suppliers use RFID at the carton and unit level to track shipments.

Third, companies that ship high-value goods, for which there are established gray and black markets, are also demanding improved security. Examples include Hewlett-Packard for computers, Intel for chips, and Pfizer for pharmaceuticals (Sheridan 2004).

Also, C-TPAT enlists shippers and retailers, with specialized security recommendations for the business supply chain (CBP, 2004).

The Logistics Layer: A Multimodal Physical Network for the Transport of Cargo

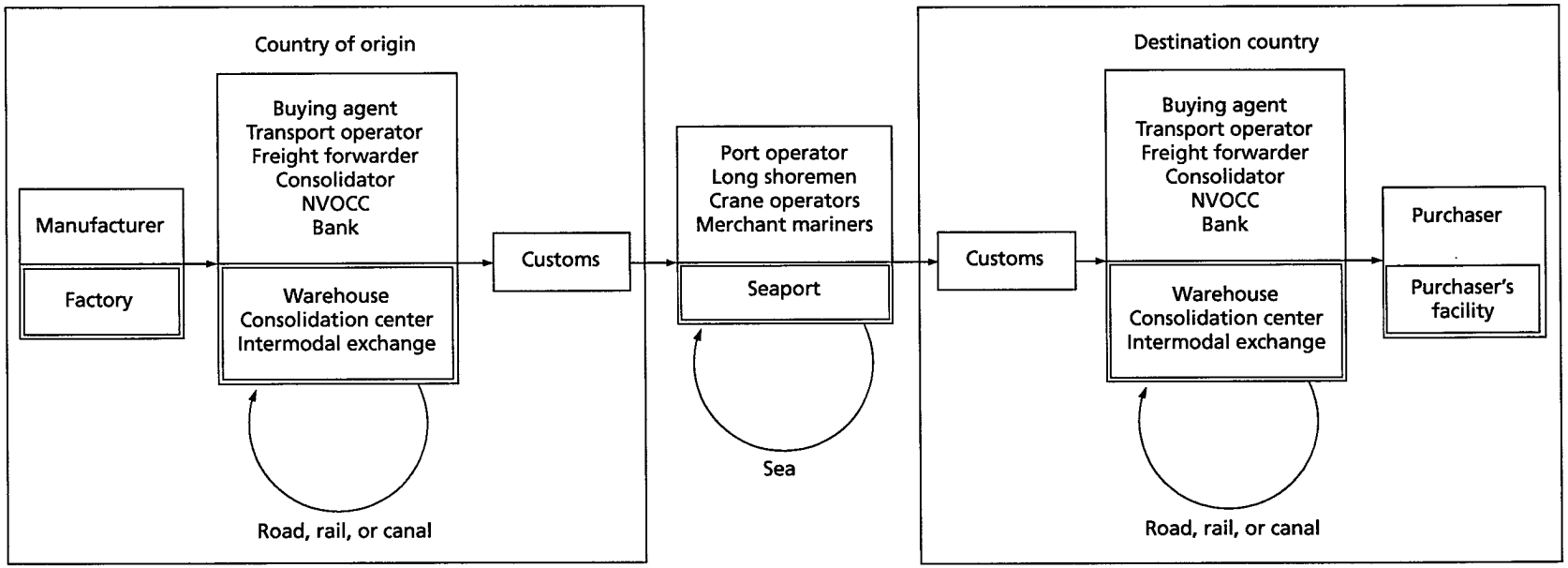
The supply chain can also be viewed as the physical system on which goods travel. This point of view is shared by those who operate the supply chain as a business: trucking companies, rail freight firms, ocean carriers, the International Labor Organization and the International Longshore and Warehouse Union, freight forwarders and consolidators, etc. This view of the supply chain merges two perspectives illustrated in a report written for OECD. In OECD (2003), author Philippe Crist considered the supply chain from the points of view of the places through which cargo travels and of the people who have access to cargo at various stages. These two perspectives are better considered together, since cargo does not move autonomously. Figure 2 consolidates two figures from OECD (2003), illustrating the movement of cargo in terms of the persons who have access to it (single-lined boxes) and by the places to which it travels (double-lined boxes and arrows). Actions to secure the supply chain follow these figures by limiting the access of people to the cargo or by securing the routes and conveyances on which it travels.

Merging the two figures allowed us to build on Crist's analysis. In particular, we should understand that the system comprises many self-similar layers: Participants fundamentally perform the function of receiving goods from one carrier and passing them along to the next; each is both a "customer" and a "supplier" (Nishiguchi and Beaudet, 2000). Therefore, the linear progression illustrated in Figure 2 is more accurately viewed as a web of directed connections among producers and consumers. Within each transport mode, there is a network of paths and nodes through which goods can travel. A shipment from a supplier to a consumer may take a number of different paths, with the paths dependent on such factors as the weather and potential security obstacles. The figure depicts these varied paths as feedback loops.

Failure of the shipping network may have more drastic consequences than it would for other infrastructure networks. Fundamental differences affect the applicability of recent results in network theory to the roadway, rail, and port terminal networks that form the global supply chain. In social, information, and certain physical networks, the flow over the network is instantaneous or nearly so. If an Internet router fails, packets are rapidly redirected along an alternative path, avoiding the fault. Some networks are able to operate despite the loss of many nodes (Amaral et al., 2000). But if a port should be closed because of a terrorist attack or, more commonly, because of an accident or spill, rerouting land and sea traffic to avoid the disruption carries significant delays and costs. For perishable food items, for example, delays can result in total loss of cargo value. Further analysis is required to determine the costs of rerouting container traffic around failed nodes and edges.

The majority of initiatives designed to increase the security of the global supply chain have focused on securing the nodes of the network, particularly seaports. A typical seaport capable of handling container traffic will service or house most of the relevant stakeholders, including the CBP, the USCG, freight forwarders and customs brokers, and ocean carriers, and will have links to the rail and highway networks. Unfortunately, seaports are also hubs, in which the road, rail, and sea networks have a common connection. MTSA (2002) and the International Ship and Port Security code of IMO focus their initiatives on measures to improve port security (OECD, 2003). These measures include the designation of an officer

Figure 2
The Logistics Layer in Terms of the Systems and People that Move Cargo. This figure combines two figures from OECD (2003), illustrating the movement of cargo in terms of the persons who have access to it (single-lined boxes) and by the places to which it travels (double-lined boxes and arrows). Actions to secure the supply chain follow these figures by limiting the access of people to the cargo or by securing the routes and conveyances on which it travels.



RAND TR214-2
SOURCE: OECD, "Security in Maritime Transport: Risk Factors and Economic Impact," Maritime Transport Committee report, 2003. Online at http://www.oecd.org/home/ (as of November 5, 2003). Adapted and used with permission.

responsible for port security and the design and approval of a port security plan. Port access controls and worker identification and background checks are also required: Mariners who wish to disembark at a U.S. port must hold a D-1 visa including a biometric identifier (Lloyd's List, 2004), and TSA is developing an identification card for all transportation workers (TSA, 2004).

Other initiatives seek to guarantee the security of containers en route. MTSA and the International Ship and Port Security code also specify the designation of vessel security officers and vessel security plans in hopes of maintaining the container's security as it travels along an edge of the network. CSI stations CBP personnel in foreign ports to facilitate the approval of U.S.-bound containers, on the assumption that the edge—the sea-lane between the foreign port and the U.S. port—is secure. The C-TPAT initiative enlists carriers in promoting security among partners, including conveyance security, access controls, procedural security, and manifest security (CBP, 2004). Although voluntary, C-TPAT seeks to ensure the security of the edges of the network by enlisting the help of those who have possession of a container as it travels between nodes. C-TPAT has been criticized both for its procedures (Stana, 2004) and for the lack of resources provided for implementation (Flynn, 2004). The transportation network forming the edges of the logistics layer spans the earth, and ensuring the security of containers via direct oversight is impossible in practical terms.

Finally, new technologies may improve security in the logistics layer. Electronic seals are used to detect tampering after the containers have been filled. Active RFID technology projects transparency on the supply chain to allow tracking containers from origin to destination. X-ray and gamma-ray scanning devices allow detection of smuggling of illegal or misrepresented cargo. Remote sensors help inspectors identify hazardous cargo or weapons. Certain government programs, such as OSC, seek to speed the development and deployment of new technology to increase supply-chain security. The Smart and Secure Tradelanes initiative is a private-sector program demonstrating the effectiveness of the new technologies.

The Oversight Layer: The Legal and Regulatory Structure of the Global Supply Chain

Each transaction or movement of goods over the supply chain occurs under the auspices of a regulatory regime consisting of all the rules, regulations, and enforcement mechanisms that govern the structure and operation of the transaction and the physical layers of the supply chain. The focus of these regulations has recently shifted from safety and trade facilitation to security. Current initiatives, such as the International Ship and Port Security code and MTSA, focus on increasing access restrictions to ports and vessels and on implementing security plans based on a particular threat level. The regulatory and oversight bodies at a U.S. port include the USCG, the CBP, the U.S. Citizenship and Immigration services, and local law enforcement and emergency response agencies. The business network linking sellers to buyers has its own governing legal and regulatory structure. The import and export regulations established by U.S. trade law are enforced by the Department of the Treasury and the FTC. Banks monitor transactions and extend lines of credit to firms. A body of contract and labor law governs the production and procurement of goods. Each piece of regulatory apparatus collects information to ensure that its directives are being met, and these data together form the intelligence that allows targeting of shipments.

In the aftermath of the terrorist attacks of September 11, 2001, new regulation has focused almost exclusively on security measures. The focus on security is a dramatic shift from the previous regulatory regime, which focused on reducing fraud and smuggling, while ensuring the safety of participants in the supply chain, reducing the environmental consequences of trade (e.g., oil spills and air pollution), and collecting all relevant tariffs and duties. We do not know whether these measures have led to the neglect of previous regulatory and enforcement goals, such as the detection and seizure of illegal drugs. Furthermore, terrorism can be prevented using many of the same means used for preventing theft and smuggling because each objective requires that the system be able to control what cargo enters and leaves the system.

New security measures focus primarily on port terminals, although some provisions extend to the high seas. MTSA and its international counterpart, the International Ship and Port Security code, require port security assessments and plans, as well as vessel security plans. But the ocean mode of the system represents only a single vulnerability. Vessel security procedures are intended to protect the integrity of cargo while it is between ports and out of view, but the ocean is also one of the areas in which the ability to compromise cargo is limited to terrorist groups with considerable resources and training.

Even with increased attention on port and maritime components of container shipping, vulnerabilities remain. In the United States, the majority of containers travel to their ultimate destinations by tractor-trailer over the interstate highway system. Along this system, the ability to track an individual shipment is limited; since the highway system is open to the public, the shipment is far more vulnerable. Along the highway network, the regulatory structure is much more diffuse, and local law enforcement must concern itself primarily with public safety. Rail systems are less accessible than the highway system but suffer from similar vulnerabilities and have arguably less oversight.

Interactions Among Layers in the Supply Chain

The three points of view each form a layer of the supply chain, each of which depends on the others; we begin with the transaction layer. In the transaction layer, the movement of raw materials, work-in-progress inventory, or finished goods represents the fulfillment of an order. Figure 3 depicts a retailer, who contracts with a foreign supplier and a common carrier to deliver the goods. The carriers in the logistics layer move freight across sea, rail, and road networks. Interacting with the other layers is the oversight layer, which sets the rules under which the lower layers operate. The regulatory network specifies actions that should be taken to secure the supply chain, levies fines, and sets standards. Note that the oversight functions are diffuse: The national and regulatory agencies evolved with specific industries but are now called on to ensure security of the supply chain. For example, U.S. Customs and Border Protection is responsible for enforcing U.S. trade law in addition to ensuring the security of the containerized supply chain.

Table 1 lists some of the organizations that comprise the transaction and logistics layers and the relevant oversight bodies. Note that oversight agencies have limited influence over organizations in either the transaction or the logistics layer.

Figure 3
Interactions Between the Logistics, Transaction, and Oversight Layers of the Supply Chain. The different points of view of the supply chain can be viewed in terms of a layered set of networks. The logistics layer is responsible for the movement of cargo along a network of roads; the transaction layer orders goods and materials from a network of suppliers; and the regulatory layer specifies standards for operation within its area of authority.

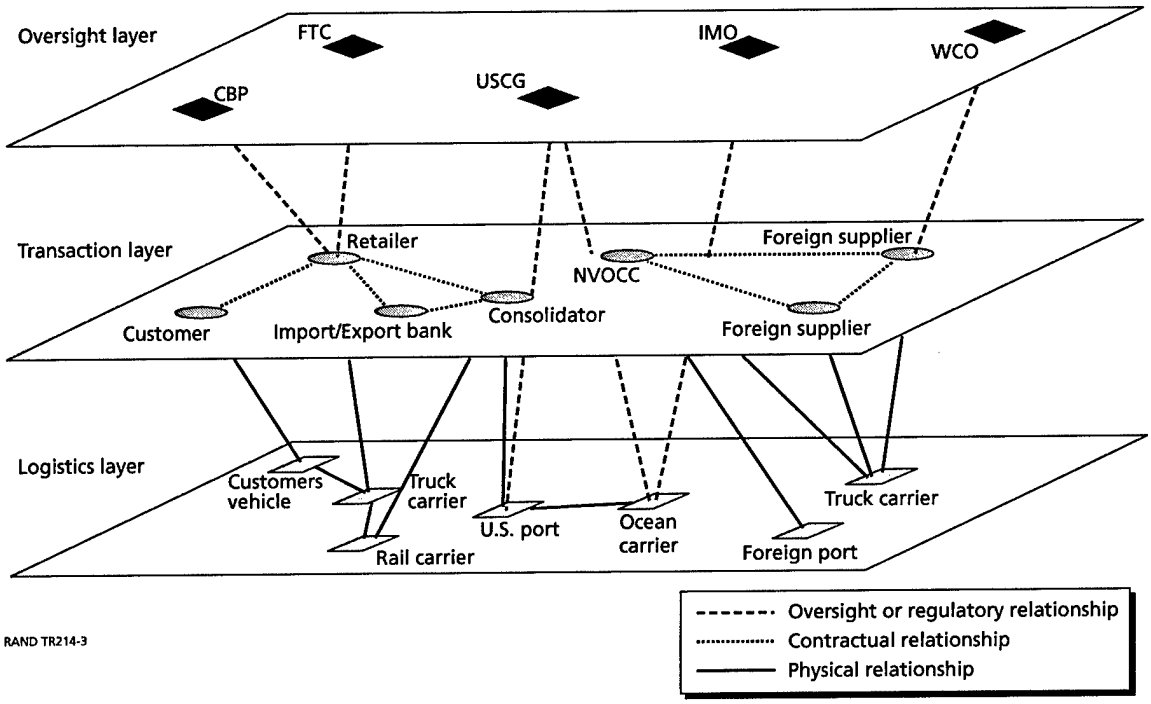


Table 1
Organizational Interests. The three layers may be specified by the organizations that comprise each layer. Note that oversight agencies have a limited range of influence over organizations in either the transaction or logistics layer.

Layer	Examples of Stakeholders	Examples of Oversight Agencies
Transaction	Wal-Mart Target Ford Non–Vessel-Operating Common Carriers (NVOCCs)	Federal Trade Commission U.S. Customs and Border Protection World Customs Organization
Logistics Layer	International Longshore and Warehouse Union Pacific Maritime Association International Labor Organization CSX Transportation APL Maersk Sealand Port of Long Beach	U.S. Department of Labor U.S. Department of Homeland Security Local law enforcement U.S. Coast Guard U.S. Customs and Border Protection World Customs Organization

Figure 3 and Table 1 also give us a method for assessing the interests of the large number of stakeholders in the system. Any organization involved in the physical movement of cargo is part of the logistics layer. The organizations responsible for staffing and operating the system that moves cargo are also part of the logistics layer. Therefore, all ocean carriers, rail freight providers, trucking companies, port operators, and their vendors (shipyards, crane works, etc.) are stakeholders in the logistics layer. The personnel and carriers are intertwined

such that the actions of one have a direct and measurable effect on the other. This is not the case for the transaction layer, for whose business the participants in the logistics layer compete—it is, after all, the freight of the Wal-Mart, Target, Home Depot, Dell Computer, Ford Motors, and others that the supply chain moves.

The layered model allows a clean demarcation of the lines of responsibility for securing the international supply chain. For example, the C-TPAT program encourages supply-chain participants to make the effort to guarantee the security of cargo and persons under its control.[6] It also obliges participants to communicate guidelines for security to supply-chain participants with whom it interacts. Companies that participate in C-TPAT receive a favorable reduction in their cargo's risk score when entering U.S. ports (United Nations Conference on Trade and Development Secretariat, 2003).

The layers in the figure illustrate domains of influence for communicating guidelines. Firms involved in the physical movement of freight are able to communicate guidelines to other physical movers most effectively, while large retailers or importers are able to communicate most effectively with their suppliers on issues of security. The C-TPAT guidelines for ocean carriers recommend procedures for vessel security, manifest preparation, and similar issues; C-TPAT guidelines for importers focus on procedures that enhance the security of cargo (CBP, 2004).

The layered model also explains the basis of objections certain groups have to particular regulations. The World Shipping Council represents the ocean carriers' interests in Washington, D.C. In September 2003, the council issued a white paper that commented on various U.S. and foreign government programs to enhance supply-chain security (World Shipping Council, 2003). The council argued that carriers were not responsible for the contents of containers, an aspect of supply-chain security over which they cannot have full control. The shipper is responsible for loading and sealing a safe and secure container. Those who have custody of the container during its transit are responsible for its security in transit. Government also has critical responsibilities and, with the support of carriers and shippers, has expanded its capabilities to gather and analyze advance data on all container shipments, screen all such shipments, and inspect any container that raises a security question (World Shipping Council, 2003).

Several initiatives implementing RFID technology limit themselves to particular layers of the supply chain. The Smart and Secure Tradelanes Initiative has enlisted large shippers in the deployment of RFID tags and readers at the container level, tracking them with handheld and crane-mounted readers at ports and on vessels (2003). This initiative therefore focuses on improving the efficiency and security of the physical supply chain. Such retailers as Wal-Mart, Target, and the Albertsons grocery store chain are also embracing RFID technology but use it to track individual products and combat counterfeiting (Feder, 2004). RFID initiatives on the part of retailers fall squarely in the transaction layer of the supply chain.

---

[6] For complete program details, see CBP (2004).

SECTION 4

Capabilities of the Global Container Supply Chain

The stability of the global container shipping industry is based on efficiency and security: Any efforts to evaluate proposals for improving this system must compare them against both these properties. This requirement holds both for new applications of technology and for proposed modifications to shipping, customs, or trade policies. The ability of a supply chain to deliver goods efficiently and securely can be represented by five capabilities:

- **Efficiency.** The global container supply chain has evolved primarily to deliver goods more quickly and more cheaply than other modes of transport when volume and mass are taken into account.
- **Shipment Reliability.** The system must behave as expected, retrieving and delivering goods as directed with a minimum amount of loss due to theft and accident. Supply-chain shrinkage, resulting from misrouting and theft of goods, erodes both this trust and the efficiency of the shipping network. Misrouting causes losses through delays in shipment delivery. Theft results in both direct economic losses and indirect losses resulting from delays in product delivery.
- **Shipment Transparency.** The goods that flow through the global container supply chain must be legitimately represented to authorities and must be legal for transport. The system should be transparent enough to minimize improper use of the system. Traditionally, transparency has involved inspections at the port of entry to detect illegal immigrants or items being smuggled in an attempt to avoid regulations or tariffs. With homeland security currently receiving so much attention, the focus of exclusion has shifted to preventing terrorists from using the container shipping system to carry out attacks on the United States. Inspection at the port of entry can make it more difficult for terrorists to use containerized shipping as logistical support for moving people and supplies. However, inspections at the port of entry are less helpful for preventing terrorists from using containers as a means of attack (e.g., detonating a bomb aboard a ship arriving at port). Increased focus on the latter capability introduces new challenges.
- **Fault Tolerance.** Because the system is a network, problems at one node—such as a port—affect interconnected parts of the system. In unstable systems, a problem at a single node or link in the supply chain can bring the entire network to a halt. In fault-tolerant systems, the surrounding ports and distribution system can compensate when a section of the system is compromised. To the extent that neighboring ports and facilities are able to compensate for the loss of a port, the containerized shipping system is more fault tolerant.

- **Resilience.** Resilience is the ability of the supply chain to return to normal operations after a failure. For example, suppose that an oil spill occurs at a port. The response to contain the spill would impede the loading and unloading of ships, creating backlogs at the port and delaying shipments elsewhere. The more resilient the supply chain is, the quicker these backlogs will be cleared, avoiding the resulting delays. Resilience is a function of the system design and the response from the oversight layer.[7]

The first three of these capabilities are characteristics of the containerized shipping system when it is functioning normally. The final two, fault tolerance and resilience, are properties of the system's response to natural or intentional disturbances. The capabilities divide between efficiency and security. Efficiency is the only capability that directly reflects the cost, speed, and capacity of the system. All other capabilities are associated with supply-chain security.

Although these capabilities will be measured through distinctly different metrics, all five capabilities are interconnected. Gains in any one capability must be assessed with respect to comparative gains or losses in the others. For example, increasing inspections may improve security but increase delays at ports. Those making decisions about the design of and investments in security policies and technologies must assess the trade-offs among the five supply-chain capabilities and consider their relative importance in the context of specific decisions.

---

[7] This is best illustrated by the Booz Allen Hamilton Port Security War Game, which estimated that closing the nation's ports for eight days would result in $58 billion in economic losses (Gerencser, Weinberg, and Vincent, 2003).

SECTION 5

Managing Container Shipping Security: A Case of Technology-Induced Risk

A secure and efficient supply chain will be the product of an interconnected system of human and technological agents. How this complex system responds under normal conditions and following severe disturbances is a case of technology-induced risk. Technology-induced risk results from the operation of technology-dependent systems. Failures occur when system components fail to operate properly, interconnections are broken, or human error compromises operations. Such failures can either be random or the result of deliberate attack.

Interventions for managing technology-induced risk influence either exposures or effects (Morgan, 1981). Efforts to reduce event occurrence or the resulting exposures are akin to threat- or vulnerability-reduction strategies. In the context of supply-chain security, these strategies translate either to reducing the probability that an attack occurs or to reducing the probability that the attack is successful. Interventions that modify or reduce effects or compensate after the fact are consequence-reduction strategies.

In addition, it is important to consider human perceptions and values because this makes it possible to prioritize terrorism risks. It is also normatively preferable to direct preparedness resources toward the hazards about which society is most concerned. In addition, understanding society's perceptions and values presents opportunities (albeit limited) for reducing risks through public education and risk communication (Morgan, 1981). Given the potential trade-offs between security and efficiency, perceptions and values determine how much disruption of the container shipping system for the sake of improved security is acceptable .

Building Supply-Chain Capabilities

Stakeholders in the containerized shipping system have proposed multiple means of improving the system's security and efficiency. Several of these were introduced in Section 2. Some proposals are regulatory or policy fixes (such as C-TPAT and CSI) that impose administrative requirements through the customs inspection process. Others, such as MTSA, impose regulatory constraints on the system. Finally, shippers, carriers, customs organizations, and port operators are also looking for technological solutions for improving container security and efficiency, such as antitamper seals, RFID, x-ray and gamma-ray scanners, and remote sensors. The layered description of the global container shipping supply chain discussed in Section 3 and the supply-chain capabilities discussed in Section 4 provide a framework for assessing how these security measures are affecting the performance of the container shipping system. Working within this framework, the remainder of this section assesses the

programs covered in Section 2 from the perspective of technology-induced risk management. Table 2 summarizes this assessment.

As an example, consider deterrence, which plays an important role in the design of all policy and technology proposals for improving security. Each proposal is designed to make it more difficult to attack the containerized shipping system. The intended result is that targeting container shipping will be less attractive for thieves, smugglers, and terrorists. In this way, deterrence contributes to threat and vulnerability reduction. Deterrence, as discussed above, is not considered further in the following descriptions. However, it does play an important role in the design of each program.

Table 2 also offers a high-level view of how these objectives come together as an integrated strategy for port security strategy and whether there are any obvious gaps in the U.S. strategy. The table presents the capabilities that could be captured by private shippers, carriers, and port operators and the U.S. government; it does not highlight security benefits that might be realized at foreign ports. Also, this analysis does not answer the question of whether the aggregate response is sufficient. Further analysis, built on our framework, is required to address this question.

Customs-Trade Partnership Against Terrorism: Making Supply-Chain Participants Responsible for the Security of Container Cargo

C-TPAT is intended to improve efficiency through implementing processes and standards for participants in the transaction and logistics layers. Although C-TPAT is mandated by the Department of Homeland Security (i.e., the oversight layer), it is driven by requirements for the other layers.

As reflected in Table 2, C-TPAT does not make any clear contributions to supply-chain security aside from deterrence. In some cases, C-TPAT may make it more difficult for illicit cargo to be shipped via containers. However, this effect may be offset by the ability of terrorists and smugglers to game the system. This "carnival booth" effect has been described with respect to TSA's computer-assisted passenger prescreening system (Martonosi and Barnett, 2004). C-TPAT also does not help reduce effects of events or mitigate them when theft, fraud, or terrorism occurs.

Operation Safe Commerce: Harnessing Technology to Improve Customs Inspection Effectiveness

OSC is an example of the oversight layer working with the logistics layer to improve supply-chain security at U.S. ports. Because OSC primarily addresses container screening and tampering technologies, it is not driven by the transaction layer.

This program might reduce fraud by improving detection at the port of entry. Similarly, Table 2 indicates that OSC might make it difficult for terrorists to use containerized shipping to supply comrades in the United States. However, OSC will not reduce the damage from a terrorist act, if an attack on the system is successful.

By the time containers reach ports, they are positioned for a terrorist attack. Thus, increased inspections will not reduce the exposure to or reduce the damages from attacks on

Table 2
Examples of How Preparedness Strategies May Influence the Exposure-Effects Chain of Notional Terrorist Events

			Anticipated Supply Chain Security Effects			
			Threat or Vulnerability Reduction		Consequence Reduction	
Policy or Technology	Driving Layer	Anticipated Supply Chain Efficiency Effects	Reduce Probability of Attack	Reduce Probability of Successful Attack	Avoid or Modify Attack Consequences	Mitigate or Compensate for Consequences
Customs-trade partnership against terrorism	Transaction and logistics	Reduced shipping cost and time and increased volume: *Expedited customs*	Reduced damage, losses, and fraud: *Deter terrorists, thieves, and smugglers*			
Operation Safe Commerce	Logistics and oversight			Reduced fraud: *Detect at entry*		
Container security initiative	Oversight			Reduced damage and fraud: *Detect at origin*		
Maritime Transportation Security Act of 2002	Oversight			Reduced theft: *Control access*		Increased Fault tolerance and resilience: *Disaster planning*
Anti-tamper seals	Transaction and logistics			Reduced damage: *Detect at origin* Reduced fraud: *Detect at origin or entry*		
Radio frequency identification	Transaction and logistics	Reduced shipping cost and time: *Improved Logistics*		Reduced theft losses: *Detect unapproved transport* Reduced damage: *Detect at origin* Reduced fraud: *Detect at entry or origin*		Increased resilience: *Rapid location and rerouting of shipments following a disaster*
X-ray and gamma-ray inspection	Logistics and oversight			Reduced damage: *Detect at origin* Reduced fraud: *Detect at origin or entry*		
Radiation pagers, portal sensors, and remote monitoring	Logistics and oversight			Reduced damage: *Detect at origin*	Reduced damage: *Detection before cargo enters ports*	

port facilities. Similarly, OSC does not reduce or modify the consequences of terrorist attacks or smuggling incidents if they are successful. Neither does it provide for compensation or mitigation to lessen the impact of losses from fraud, terrorism, or theft.

Container Security Initiative: Increasing Deterrence and Efficiency Through Cargo Inspection at Foreign Ports

CSI, an oversight-driven program, clears U.S.-bound containers at foreign ports. By increasing detection capabilities at the port of origin, CSI might improve the likelihood of detecting threats before they are onboard a ship bound for the United States. Thus, CSI could reduce U.S. exposure to losses from fraud and terrorism damage. This program might also reduce the processing time required at domestic ports of entry. However, because the program could increase processing time at the port of origin, it is not clear that a net improvement of efficiency will result.

Since CSI is solely focused on increased detection capabilities, Table 2 shows that it does not help decrease the effects of system hardening or mitigate the consequences of attacks.

Maritime Transportation Security Act: Reducing Theft and Improving Incident Response at Ports and on Vessels

MTSA is the response of the oversight layer to the threat of terrorist attack on the ports or U.S. vessels. Standardized port security and inspection protocols can reduce the costs of theft by controlling access to containers during transport. However, control at the port of entry will not reduce potential damages from terrorist attacks on ports from inbound containers. Making emergency response part of the port security plans can help increase the fault tolerance and resilience of the containerized shipping system.

None of MTSA's requirements clearly help improve the efficiency of the supply chain (see Table 2). In fact, the shipping industry has expressed some concern that its measures will increase shipping costs. In addition, MTSA does not institute measures that would affect the causes of damage or reduce the effects of theft, fraud, or terrorism.

Antitamper Seals: Improving the Integrity of Container Shipping

The transaction and logistics layers have driven the adoption of antitamper seal technology; the oversight layer has not mandated such technologies. As Table 2 indicates, antitamper seals might increase detection capabilities at ports of origin and ports of entry. Detecting tampering at the port of origin reduces the potential for damage to a U.S. port from either fraud or terrorism. Detection at ports of entry reduces only the potential damage from fraud. However, it is possible to breach a container without damaging many of the seals, thus circumventing the technology.

Antitamper seals are not intended to have significant effects on supply-chain efficiency. Any reductions in inspection or processing time would likely be modest and would

have to be balanced against the costs of the antitamper devices themselves. Antitamper seals will not modify the causes or help mitigate or compensate for effects when events do occur.

Radio Frequency Identification: Improving the Transparency of Supply-Chain Networks

As with antitamper seal technology, the transaction and logistics layers are driving adoption of RFID technology. However, unlike antitamper seals, RFID technology is expressly intended to increase efficiency.

RFID technology, as shown in Table 2, is intended to make the supply chain transparent, allowing carriers and shippers to track shipments from origin to destination. Through network transparency, shippers might see where bottlenecks occur in their supply chain and could potentially optimize shipping to improve supply-chain efficiency. Transparency can reduce the costs of theft and lost goods through early detection of misrouted or unapproved goods. Detection of inconsistencies in container contents, when observed at the port of origin, reduces both terrorism damage and fraud. Detection at the port of entry can decrease losses from fraud.

RFID also contributes to consequence reduction. Although RFID is not expected to modify the causes of effects, the ability to locate and reroute shipments rapidly following disasters improves supply-chain resilience.

X-Ray and Gamma-Ray Scanning: Improving Transparency of Cargo Shipments

Participants in the oversight layer have been the primary driver for scanning technologies, in an effort to keep dangerous goods out of the supply chain and to detect illegal cargo.

Using scanning technologies at foreign ports might reduce both losses from fraud and terrorism damage in the United States (see Table 2). Detection at the port of entry fundamentally reduces losses from fraud, although it may also reduce potential damage from terrorism significantly. For example, if a container is carrying a weapon intended for a specific target in the U.S. interior, detecting that weapon at the port of entry would allow it to be isolated and thus reduce the chance of significant damage.

Container scanning is not expected to improve supply-chain efficiency. In fact, scanning adds time to the processing of containers, and port operators or customs inspectors must bear the costs of the scanning equipment. Similarly, container scanning is not expected to help reduce consequence reduction because scanning does not mediate the effects of successful acts of terrorism.

Radiation Pagers, Portal Sensors, and Remote Monitoring: Increasing Capabilities to Detect Weapons of Mass Destruction

The oversight layer has also driven the adoption of remote-sensing technologies, such as radiation-warning pagers, portal radiation sensors, and remote-monitoring technologies. These systems detect radiation—new technologies may detect other agents—as the container

travels through the system. Detection at any point in the system hinders terrorists' ability to use container shipping as a weapon. However, as indicated in Table 2, detection must occur before containers reach the port of entry to prevent damage from attacks on the United States.

Improving detection capabilities at the port of origin provides the most significant reduction of potential terrorism damage to the United States. In addition, remote sensors that can detect weapons of mass destruction on ships before they reach port can also reduce terrorism damage.

Development of appropriate remote screening or portal sensors might also contribute to the detection of drugs or other misrepresented or illicit cargo. Currently, attention is mainly on the development of sensors for weapons of mass destruction. Sensors are not anticipated to improve supply-chain efficiency and do not mitigate or compensate for damages or losses when events do occur.

SECTION 6

Preliminary Conclusions, Recommendations, and Future Inquiry

The global containerized supply chain is omnipresent. Thus, terrorist attacks on or using the supply chain could occur anywhere, and a well-planned attack could result in significant loss of life. In addition, the U.S. economy depends on the continued operation of the containerized supply chain: A successful attack on the supply chain could cause billions of dollars in damage to the U.S. economy (OECD, 2003; Pollack 2004). The threat of terrorist attacks using the container shipping system therefore demands policy attention.

The security of the supply chain can be considered a public good. Some who have not invested in these port security systems are likely to profit from the systemwide benefits (such as deterrence of terrorists and smugglers). It is not possible to prevent them from doing so, but their doing so does not diminish the benefits to those who did invest in the systems. On the other hand, this creates "free-rider" problems: Because those who do not invest will still benefit, the private sector may end up underinvesting in security. It may therefore be appropriate for government to step in to ensure the security of the global supply chain.

To this end, this report has developed a capabilities-based framework for assessing the security of the supply chain and determining areas where gaps in security remain. Our analysis has revealed some preliminary results and recommendations, as well as insights into several areas for further investigation.

Preliminary Conclusions

The analysis of supply-chain security and current efforts to improve it presented in the previous chapters leads to two conclusions. First, supply-chain efficiency and security are distinct but interconnected. Efforts to improve supply-chain efficiency may or may not affect the security of the system. Second, both public- and private-sector initiatives to improve the security of the global supply chain have focused largely on the prevention and deterrence of smuggling and terrorist attacks. Few initiatives have focused on improving the fault tolerance or resilience of the system.

The Inseparability of Supply-Chain Security and Efficiency

Improving the supply-chain's efficiency may or may not improve its security. Increasing transparency to improve efficiency may also improve supply-chain security. Labor reductions for the sake of efficiency, however, may decrease security. Similarly, proponents of increased supply-chain security often cite increased efficiency as an auxiliary benefit, although the two properties are often independent. Other measures, such as increased inspections, could create delays that would lead to losses of perishable cargo or to negative economic effects on con-

signees. The interconnected nature of supply-chain capabilities suggest that security measures that reduce efficiency could have unintended negative consequences because stakeholders will look for ways to compensate for or circumvent the security requirements.

Specific examples abound. Product theft is a business risk for all users of the supply chain, and shippers and carriers have instituted policies to combat it. But the benefits of increased oversight and monitoring required to combat theft, or the processes recommended by CBP in the C-TPAT program, do not necessarily increase the efficiency of the supply chain.[8] Actions that combat smuggling, likewise, have little effect on supply-chain efficiency; the smuggler's activities occur alongside normal business practices. Improving the two other properties of the supply chain, fault tolerance and resilience, does not increase efficiency and, under normal operating conditions, might work against it. Both these properties imply a certain amount of spare capacity, particularly at port terminals but also on ships and at transshipment points. Spare capacity, under normal operating conditions, is a misallocation of resources.

Potential Underinvestment in Fault Tolerance and Resilience

Most initiatives for securing the supply chain are public-sector efforts, focusing disproportionately on preventing terrorist attacks. In response to the attacks of September 11, 2001, CBP now views its primary role as fighting terrorism (Jacksta, 2004). Before then, CBP's principal regulatory roles were collecting duties and preventing smuggling.

Our analysis shows that few security enhancement programs seek to ensure either the fault tolerance or resilience of the system. As mentioned previously, these capabilities are a function of both the system design and the responses of participants in the oversight layer. In principle, it is in the best interests of a firm to plan for supply-chain failures. However, at the logistical level, additional capacity is incredibly capital intensive, and carrying it on a balance sheet makes little business sense.[9]

In 2002, the Port of Los Angeles and the Port of Long Beach handled 70 percent of all west-coast container traffic (Pacific Maritime Association, 2003). This concentration is a vulnerability created by the system's drive for efficiency. Were both ports to close for security reasons, the other west-coast ports, combined, lack the necessary infrastructure for absorbing all the traffic calling at Los Angeles and Long Beach. And they should not. However, incentives for development at smaller ports would create redundancy and excess capacity that would improve the fault tolerance and resilience of the container shipping system during an emergency. Because these incentives do not exist and receive little attention from members of the transaction or logistic layers, public investment will be needed to provide fault tolerance and resilience.

---

[8] Since shipments and containers belonging to C-TPAT participants are granted expedited processing and clearance at U.S. ports of entry, CBP argues that the program increases supply-chain efficiency (Ginn and Lacy, 2004). This argument is misleading; participation in C-TPAT reduces the risk score that triggers an inspection but does not uniformly decrease the transit or dwell times of containers.

[9] A Dutch Telematica Institut study assumed that logistical operations are already optimized for efficiency because they are so capital intensive (Goedvolk et al., 2001).

Recommendations

These conclusions suggest three complementary paths for improving the security of the global container supply chain while maintaining its efficiency.

The Public Sector Should Seek to Bolster the Fault Tolerance and Resilience of the Logistical Supply Chain

The logistics level of the supply chain has distinctly private and public components: Ports are operated by private firms, such as P&O Nedlloyd and Hutchinson Port Holdings, and by port authorities; the freight rail network is largely privately owned and operated; and the interstate highway system is distinctly public. The closure of a major port—for whatever reason—would have a significant effect on the U.S. economy, and it is important to recognize that an appropriate response includes rerouting cargo to other available ports on some optimum basis and making plans for returning to normal operation. The government should lead the coordination and planning for such events for two reasons: First, the motivation of the private sector to allocate resources to such efforts is subject to the market failures of providing goods to the public; second, the government will be responsible for assessing security and decisions to close ports.

Security Efforts Should Address Vulnerabilities Along Supply-Chain Network Edges

Current efforts to improve the security of the supply chain focus on ports. MTSA and International Ship and Port Security codes specify a number of measures for controlling access to port facilities, monitoring the port area, and preparing for various emergency scenarios. Unfortunately, the route over which cargo travels is vast and difficult to secure, and many ports around the world had failed to follow the International Shipping and Port Security guidelines by the July 1, 2004, deadline. Tamper-evident seals and alarms can help identify compromised shipments, but, depending on the trade route, days or weeks may elapse before intrusions are detected. It is technologically possible to monitor the movement of all shipments in real time. Even though it is impossible to identify all illegal activity occurring in the supply chain, continued development of technologies to monitor network edges will help fill an important gap in the layered approach to container security.

R&D Should Target New Technologies for Low-Cost, High-Volume Remote Sensing and Scanning

Current sensor technologies for detecting weapons or illegal shipments are expensive and typically impose delays on the logistics system. As a result, security efforts have focused on technologies or processes for identifying containers that have been tampered with, for making it harder to tamper with containers, and for profiling containers to reduce the burden of volume on screening systems.

All these approaches have a common weakness: They are easy to circumvent. Tamper-resistant seals can be fooled. Profiling processes can be gamed as terrorists or smugglers learn what characteristics trigger profiling algorithms. New detection technologies for remote scanning of explosives and radiation would provide valuable capabilities for better securing the container shipping system. Technology planning must also be coordinated with market requirements for developing devices with low development and deployment costs.

Future Inquiry

This document is our initial assessment of the security of the global supply chain; we are continuing our work in several areas:

1. **Assessment of policies for improving supply chain security.** We have described a framework for assessing supply-chain security using a set of interrelated performance dimensions and a layered structure of the supply chain. The framework is readily applied to domestic and international policies and proposals, providing a consistent approach to evaluating their performance and security implications. Additionally, since the performance dimensions of fault tolerance and resilience are properties of the system as a whole, the framework allows quantitative assessment of appropriate public and private sector roles in protecting the supply chain.
2. **Systems analysis of supply-chain risk.** Modern business practices and the physical structure of the containerized supply chain conspire to amplify disruptions to the system. The framework described in this document can be applied to analyze sensitive nodes in the system and its critical paths, evaluate the systemwide effects of the adoption of new technologies, and determine procedures for "restarting" the system in the event that it must be shut down for security reasons.
3. **Technology assessment and research and development planning for improving supply-chain performance.** Research, development, and deployment programs continue for new technologies to improve supply-chain performance. The potential of these technologies to change the performance dimensions of the supply chain may now be evaluated; conversely, with knowledge of desired performance improvements, research and development planning may be undertaken to achieve them.
4. **Economic analysis of global trade trends in supply-chain performance.** The global supply chain is protean, and the roles of producing and consuming nations continue to shift. Extensions of this analysis include examining the competitiveness of particular trade lanes given regulatory changes to improve security and the study of the information flows among the transaction, logistics, and oversight layers required to support global trade and security.

References

Alling, Philip, Edward M. Wolfe, and Scott D. Brown, *Compliance Deadlines Loom: Supply-Chain Giants Drive Early Adoption of RFID*, New York: Bear-Stearns Equity Research, 2004.

Amaral, L. A. N., A. Scala, M. Barthelemy, and H. E. Stanley, "Classes of Small-World Networks," *Proceedings of the National Academy of Science*, Vol. 97, No. 21, 2000, pp. 11149–11152.

CBP—*See* U.S. Customs and Border Protection.

Cleeland, Nancy, Evelyn Iritany, and Tyler Marshall, "Scouring the Globe to Give Shoppers an $8.63 Polo Shirt," *Los Angeles Times*, November 24 , 2003, p. A1.

Cohen, Stephen S., *Economic Impact of a West Coast Dock Shutdown*, Berkeley, Calif.: University of California, 2002.

Feder, Barnaby J., "Wal-Mart Hits More Snags in its Push to Use Radio Tags to Track Goods," *The New York Times*, March 29, 2004, p. C4.

Flynn, Stephen E., "Beyond Border Control," *Foreign Affairs*, Vol. 79, No. 6, 2000, p. 57.

———, *America the Vulnerable*, New York: Harper Collins, 2004.

Ford, L. R., Jr., and D. R. Fulkerson, *Flows in Networks*, Princeton, N.J.: Princeton University Press, 1962.

General Accounting Office, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*, Washington, D.C., GAO-03-770, 2003.

Gerencser, Mark, Jim Weinberg, and Don Vincent, *Port Security War Game: Implications for U.S. Supply Chains*, McLean, Va.: Booz Allen Hamilton, 2003.

Ginn, Michael, and Tamara Lacy, "An Overview of CSI and C-TPAT," paper presented at Maritime Homeland Security 2004, March, Miami Beach, Fla., March 29–31, 2004.

Goedvolk, Ernst-Jan, Bob Hulsebosch, Wil Janssen, and Piet Maclaine, *Risk Analysis of Container Import Processes: Security Risks Associated With Flows of Goods and Information in the Port of Rotterdam*, Version 1.2, Enschede, The Netherlands: Virtuele Haven, Telematica Institut, 2001.

Guare, John, *Six Degrees of Separation*, play, New York: Vintage, 1990.

Holmes, Bruce J., *Transportation Network Topologies, Network Theory: A Primer and Questions for Air Transportation System Applications*, Washington, D.C.: National Aeronautics and Space Administration, 2004.

IMO—*See* International Maritime Organization.

International Maritime Organization, Web site, 2004. Online at http://www.imo.org/ (as of October 15, 2004).

Iritany, Evelyn, and Marla Dickerson, "Calculating Cost of West Coast Dock Strike is a Tough Act," *Los Angeles Times*, November 26, 2002.

Jacksta, Robert, "An Overview of U.S. CBP's Role in Maritime Homeland Security," paper presented at Maritime Homeland Security 2004, Miami Beach, Fla., 29–31 March, 2004.

Lloyd's List, When Security on Shore Compromises Safety at Sea, online broadsheet, April 28, 2004.

Machalaba, Daniel and Bruce Stanley, "In California, Santa's Goods Face Port Delays," *Wall Street Journal*, October 14, 2004, pp. B1–B2.

Martonosi, Susan E., and Arnold I. Barnett, "Security Profiling of Airline Passengers: How Effective Would It Be? Some Surprising Conclusions," working paper, Cambridge, Mass.: Massachusetts Institute of Technology, 2004.

Morgan, M. Granger, "Probing the Question of Technology-Induced Risk," *IEEE Spectrum*, Vol. 18, No. 11, 1981, pp. 58–64.

Nishiguchi, Toshihiro, and Alexandre Beaudet, "Fractal Design: Self-organizing Links in Supply Chain Management," in G. Von Krogh, I. Nonaka and T. Nishiguchi, eds., *Knowledge Creation: A Source of Value*, London: Macmillan, 2000.

Organisation for Economic Co-Operation and Development, "Security in Maritime Transport: Risk Factors and Economic Impact," Maritime Transport Committee report, 2003. Online at http://www.oecd.org/home/ (as of November 5, 2003).

Pacific Maritime Association, *Annual Report*, San Francisco, Calif.: Pacific Maritime Association, 2002.

———, *Annual Report*, San Francisco, Calif.: Pacific Maritime Association, 2003.

Pelosi, Nancy, and Tom Daschle, "Pelosi and Daschle Deliver Pre-Buttal to State of the Union Address," Washington, D.C.: U.S. Senate, Office of the Democratic Leader, January 16, 2004. Online at http://democrats.senate.gov/~dpc/releases/2004116B38.html (as of October 26, 2004).

Pollack, Richard, *The Colombo Bay*, New York: Simon and Schuster, 2004.

Sheridan, Ralph, Interview regarding container security initiatives, Arlington, Virginia, 21 July, 2004.

Simchi-Levi, David, Philip Kaminsky, and Edith Simchi-Levi, *Designing and Managing the Supply Chain*, 2nd ed., New York: McGraw-Hill/Irwin, 2002.

Smart and Secure Tradelanes, "Phase One Review, Network Visibility: Leveraging Security and Efficiency in Today's Global Supply Chains," November 2003.

Stana, Richard M., "Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection," testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, Washington, D.C.: General Accounting Office, GAO-04-557T, 2004.

Technology Asset Protection Association, Web site, 2004. Online at http://www.tapaemea.com (as of October 15, 2004).

Transportation Security Administration, Operation Safe Commerce, Web page, 2004. Online at http://www.tsa.gov/public/interapp/asset_summary/asset_summary_0122.xml (as of October 15, 2004).

———, "TSA to Test New ID Card for Transportation Workers," press release, August 10, 2004. Online at http://www.tsa.gov/public/display?theme=44&content=09000519800c10bd (as of October 15, 2004).

U.N. Conference on Trade and Development Secretariat, Container Security: Major Initiatives and Related International Developments, 2003. Online at http://www.unctad.org/Templates/webflyer.asp?docid=4481&intItemID=1397&lang=1 (as of October 15, 2004).

U.S. Congress, 2002, Maritime Transportation Security Act, Public Law 107-295.

U.S. Customs and Border Protection, Enforcement: International Activities, Web site, undated. Online at http://www.cbp.gov/xp/cgov/enforcement/international_activities/csi (as of October 15, 2004).

———, Import: Commercial Enforcement, Customs-Trade Partnership Against Terrorism, Web page, 2004. Online at http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/ (as of October 15, 2004).

Wasem, Ellen, Jennifer Lake, Lisa Seghetti, James Monke, and Stephen Viña, *Border Security: Inspections Practices, Policies, and Issues*, Washington, D.C.: Congressional Research Service, 2004.

Watts, Duncan J., "Small Worlds: The Dynamics of Networks Between Order and Randomness," in P. W. Anderson, J. M. Epstein, D. K. Foley, S. A. Levin, and G. Meayer-Kress, eds., *Princeton Studies in Complexity*, Princeton, N.J.: Princeton University Press, 1999.

Wolfe, Edward M., Philip Alling, Harry D. Schwefel, and Scott D. Brown, *Track(ing) to the Future: The Impending RFID-Based Inventory Revolution*, New York: Bear-Stearns Equity Research, 2003.

World Shipping Council, *In-Transit Container Security Enhancement*, Washington, D.C.: World Shipping Council, 2003.